

CLAIMS:

1. Method of communicating a communication fragment (211), the communication fragment comprising a first target address reference referring to a group of at least one receiver device (203), comprising the steps of:
 - a sender device (201) adding a cryptographic message integrity code to protect
5 at least part of the communication fragment,
 - the sender device transmitting the protected communication fragment to a router device (202),
 - the router device, for at least one receiver device in the group of target devices, modifying the first target address reference into an address of the at least one receiver device,
10 while maintaining the unchanged cryptograph message integrity code, and subsequently forwarding the modified protected communication fragment (213) to the at least one receiver device,
 - the at least one receiver device receiving the modified protected communication fragment,
 - 15 - the at least one receiver device restoring the original protected communication fragment in order to allow verification of the original protected communication fragment using the message integrity code.
2. Method according to claim 1, wherein the first communication fragment
20 comprises a bit field IA to indicate whether indirect addressing is used.
3. Method according to claim 1, wherein the sender device and the at least one receiver device share a common cryptographic key, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key.
25
4. Method according to claim 3, wherein the common cryptographic key is used to encrypt the message content.

5. Method according to claim 1, wherein the at least one receiver device restores the original protected communication fragment by substituting the first target address reference with each of the group identities that comprises the sender device to determine for which of the group identities the message integrity code matches.

5

6. Method according to claim 1, wherein

- the router device, in the step of modifying the first target address reference, stores the first target address reference in the modified protected communication fragment, and

10 - the at least one receiver device restores the original protected communication fragment using the stored first target address reference in the modified protected communication fragment in order to allow verification of the message integrity code.

7. Sender device (201) being arranged to transmit a communication fragment through a router device (202) towards a receiver device (203), the communication fragment (211) comprising a first target address reference referring to a group of at least one receiver device, the sender device comprising:

15 - protecting means (221) being arranged to add a cryptographic message integrity code to protect at least part of the communication fragment, and
20 - transmitting means (222) being arranged to transmit the communication fragment to a router device that is not able to modify the cryptographic message integrity code.

8. Router device (202) being arranged to route a communication fragment (211) from a sender device towards a receiver device, the communication fragment comprising a first target address reference referring to a group of at least one receiver device, the router device comprising:

25 - receiving means (223) being arranged to receive the communication fragment, comprising a first address reference referring to a group of at least one receiver device, the
30 first communication fragment at least partly being protected by a MIC,
- modifying means (224) being arranged to modify the communication fragment, by replacing the group of at least one receiver device by a reference referring to the at least one receiver device, while maintaining the original MIC, and

- transmitting means (225) to transmit the modified communication fragment (213) to the at least one receiver device.

9. Receiver device (203) being arranged to receive a modified communication fragment (213) originating from a transmitter device through a router device, the modified communication fragment being derived from a communication fragment (211) comprising a first target address reference referring to a group of at least one receiver device, the receiver device comprising:

- receiving means (226) being arranged to receive the modified communication fragment,
- restoring means (227) being arranged to restore the original communication fragment that was used to compute the cryptographic message integrity code, and
- verification means (228) being arranged to verify the cryptographic message integrity code.

10. System (200) for communication comprising a sender device (201), router device (202), and receiver device (203) as described in claims 7, 8 and 9.

11. Signal for secure indirect addressing, comprising a modified communication fragment (213) according to the method of claim 1.